PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/EP2005/002162	28.02.2005	02.03.2004

International Patent Classification (IPC) or both national classification and IPC
INV. H04L9/32

Applicant
FRANCE TELECOM

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA"). However, this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of three months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA:

European Patent Office - Gitschiner Str. 103
D-10958 Berlin
Tel. +49 30 25901 - 0
Fax: +49 30 25901 - 840

Authorized Officer

Carnerero Álvaro, F

Telephone No. +49 30 25901-469

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/EP2005/002162

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

   ☐ This opinion has been established on the basis of a translation from the original language into the following language , which is the language of a translation furnished for the purposes of international search (under Rules 12.3 and 23.1(b)).

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

   a. type of material:

   ☐ a sequence listing

   ☐ table(s) related to the sequence listing

   b. format of material:

   ☐ in written format

   ☐ in computer readable form

   c. time of filing/furnishing:

   ☐ contained in the international application as filed.

   ☐ filed together with the international application in computer readable form.

   ☐ furnished subsequently to this Authority for the purposes of search.

3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-18
	No:	Claims	
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-18
Industrial applicability (IA)	Yes:	Claims	1-18
	No:	Claims	

2. Citations and explanations

see separate sheet

1. The following documents (D) are referred to in this communication; the numbering will be adhered to in the rest of the procedure:

D1: WEN-SHENQ JUANG, CHIN-LAUNG LEI, PEI-LING YU: "A Verifiable Multi-Authorities Secret Election Allowing Abstaining from Voting" INTERNATIONAL COMPUTER SYMPOSIUM, [Online] December 1998 (1998-12), pages 1-21, XP002284452 TAINAN, TAIWAN. Retrieved from the Internet: URL:http://citeseer.ist.psu.edu/cs> [retrieved on 2004-06-11]
D2: JUANG W S ; LEI C L ; LIAW H T: "Fair blind threshold signatures based on discrete logarithm" COMPUT. SYST. SCI. ENG. (UK), COMPUTER SYSTEMS SCIENCE AND ENGINEERING, CRL PUBLISHING, vol. 16, November 2001 (2001-11), pages 1-21, XP002284453. ISSN: 0267-6192

2. Document D1 discloses an electronic voting scheme which uses a threshold fair blind signature scheme in which the digital signature associated with a given voter's vote is obtained from a sufficient sub-set of a group of "admin" servers and verified with the aid of a sufficient sub-set of a group of trusted authorities ("scrutineers"), and in which the privacy and anonymity of voters is guaranteed by dint of mix-nets. See pages 1-10, 15 and 16 from D1.

2.1 For further elaboration on the "blindness" and fairness of the threshold signature scheme used in the prior art, see D2. This document is referred to on page 6 of D1 (see the PCT International Search and Preliminary Examination Guidelines, 13.12 and 13.13).

2.2 Therefore, the subject-matter of the independent claims (claims 1, 10, 15 and 17) is not inventive in the sense of Article 33(3) PCT, and the requirements of Article 33(1) PCT are not met.

3. It is not at present apparent which part of the application could serve as a basis for a new, allowable claim. Should the applicant nevertheless regard some particular matter as patentable, he or she should indicate in the letter of reply the difference of the subject-matter of an eventual new claim vis-à-vis the state of the art, as well as the significance thereof.